



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/534,857	05/13/2005	Sebastien Canard	33901-175PUS	7415

27799 7590 09/23/2009
COHEN, PONTANI, LIEBERMAN & PAVANE LLP
551 FIFTH AVENUE
SUITE 1210
NEW YORK, NY 10176

EXAMINER

VAUGHAN, MICHAEL R

ART UNIT	PAPER NUMBER
----------	--------------

2431

MAIL DATE	DELIVERY MODE
-----------	---------------

09/23/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/534,857	Applicant(s) CANARD ET AL.	
	Examiner MICHAEL R. VAUGHAN	Art Unit 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 August 2009.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4-6 and 9-21 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 1,2,4-6,9-14,20 and 21 is/are allowed.
- 6) ☒ Claim(s) 15-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 June 2009 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on **8/19/09** has been entered.

Claims 1, 4-6, 9-11, and 15 are amended. Claims 3, 7, and 8 are canceled.
Claims 1, 2, 4-6, and 9-21 are pending.

Response to Amendment

Drawings

Newly submitted drawings (filed on 6/29/09) are accepted.

Claim Rejections - 35 USC § 112

The current amendments overcome the previous 112 claim rejections.

Allowable Subject Matter

The following is a statement of reasons for the indication of allowable subject matter: Claim 1, recites the limitation "authenticating the client by producing an anonymous signature of the initialization token, the signatures being obtained using a private key associated with said public key and opening an anonymous authentication session with the server, wherein said anonymous signature is a unique signature used for said authentication session". This limitation in combination with all of the other limitations is not found in the prior art. The closest found prior art, Teper, fails to teach using an initialization token of a series of tokens as defined by the claim to produce an anonymous signature.

Claims **1, 2, 4-6, 9-14, 20, and 21** are allowed.

Response to Arguments

Applicant's arguments with respect to claims 15-19 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2431

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teper et al. (US 5,815,665) hereinafter Teper in view of Aiello et al. (US 6,397,329 B1), hereinafter Aiello.

As per claim 15, Teper teaches a system adapted to open and maintain an authentication session guaranteeing non-repudiation, wherein an anonymous signature unique to the session (col. 11, lines 27-30) and comprising a series of tokens is used to open and maintain each session (col. 9, line 60-col. 10, line 2), the system comprising:

means for implementing three stages comprising:

a first stage in which a client calculates the series of tokens (col. 9, line 67 - col. 10, line 1);

a second stage in which the client makes a strong undertaking to the server as to the series of tokens (col. 9, lines 60-62);

a third stage of maintaining the session with the aid of the series of tokens (col. 11, lines 27-30). Teper fails to teach that the series of token comprising an initialization token of the series of tokens and another token responsible for maintaining the authentication session. Aiello teaches that having to keep requesting new tokens can be excessive overhead (col. 5, lines 55-60). Aiello teaches that once a token has been generated, a new token can be efficiently generated by simply hashing the old token a

Art Unit: 2431

number of times (col. 6, lines 20-30 and col. 7, lines 25-35). This would cut down on the number of communications in Teper's system if the user would not have to keep contacting the Broker server for new tokens needed for authentication. The claim would have been obvious because combining known methods which produce predictable results is within the capabilities of one of ordinary skill in art. The combination of Aiello and Teper would create a more efficient communication. Hash functions are very efficient calculations.

As per claim 16, Teper teaches wherein the first stage calculates the series of token based on two cryptographic primitives, wherein the two cryptographic primitives are a hashing function (col. 10, lines 1-3) and a random number (col. 9, line 59).

Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teper and Aiello as applied to claim 15 and in further view of Sako.

As per claim 17, it is noted that Teper and Aiello do not explicitly teach the limitation of "using a group signature by associating a plurality of identifiers and respective private keys with a single group public key."

On the other hand, Sako teaches the abovementioned limitation (page 1, paragraph 0015) as the verification subsystem confirms that the data submitted has a signature verifiable by a group public key affixed and when the confirmation is obtained,

Art Unit: 2431

this can be regarded as the data sent by a participant subsystem belonging to an eligible group.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Teper and Aiello because use of the group signature makes it impossible to identify the particular participant in the group, which makes it possible to maintain anonymity.

With respect to claim 18, it is noted that Teper does not explicitly teach the limitation of “using a blind signature.”

On the other hand, Sako teaches the abovementioned limitation (page 1, paragraph 0005) as a participant subsystem authorized to vote proves before a manager subsystem that the presenter is authorized to vote and then has the manager subsystem sign the voting contents by section of blind signature.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Teper because since blind signature is used, even the manager subsystem cannot know to which participant subsystem the voting statement with the signature has been issued, which makes it possible to maintain anonymity.

Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Teper and Aiello as applied to claim 15 in further view of Beaver et al. (US 7,234,059 B1), hereinafter Beaver.

It is noted that Teper does not explicitly teach the limitation of “the powers to revoke anonymity is divided between two or more authorities.”

On the other hand, Beaver teaches the abovementioned limitation (column 2, lines 60-64) as in systems providing revocable anonymity, anonymity is in place unless a specified event (e.g., court order) demands it be revoked and the identity of the offender revealed. It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate the teachings of Beaver into the system of Teper and Aiello to prevent undesirable situations in which troublemakers cannot rely on anonymity to cause harm.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR.

Art Unit: 2431

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/William R. Korzuch/

Supervisory Patent Examiner, Art Unit 2431